UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

UNITED STATES OF AMERICA,	§	
	§	
Plaintiff.	§	
	§	
v.	§	CRIMINAL NO. A-19-CR-111 LY
	§	
MICHAEL EZEAGBOR,	§	
	§	
Defendant.	§	[SENTENCING: October 18, 2019]
	§	

GOVERNMENT'S MEMORANDUM IN AID OF SENTENCING

The United States, by and through its attorneys, the United States Attorneys for the Western District of Texas and the District of Columbia, hereby submits the following memorandum to assist the Court in issuing an appropriate sentence in this case. For the reasons set forth herein, the government recommends that the Court sentence the defendant to the low end of the applicable guideline range. The government further recommends that the Court sentence the defendant to 10 years of supervised release with conditions including that the defendant undergo sex offender treatment (as recommended by the United States Probation Office), the defendant's computer and internet usage be limited and monitored, and the defendant's direct contact with minors be limited and supervised.

I. BACKGROUND

On May 30, 2019, the defendant pled guilty to one count of Possession of Child Pornography, in violation of 18 U.S.C. § 2252(a)(4), before U.S. Magistrate Judge Andrew Austin in the Western District of Texas. The case had been transferred to the Western District of Texas

on May 13, 2019 from the District of Columbia. During the plea hearing, the defendant admitted the following facts, as set forth in the written Statement of Offense, to be true.

The Tor Network

Tor is a computer network which anonymizes Internet activity by routing a user's communications through a global network of relay computers (or proxies), thus effectively masking the internet-protocol ("IP") address of the user. An "IP address" is a unique numeric address (used by computers on the internet) that is assigned to properly direct internet traffic. A publically visible IP address can allow for the identification of the user and his/her location.

To access the Tor network, a user has to install freely available Tor software, which relays only the IP address of the last relay computer (the "exit node"), as opposed to the user's actual IP address. There is no practical method to trace a user's actual IP address back through those Tor relay computers.

The Tor network makes it possible for a user to operate a special type of website, called "hidden services," which uses a web address that is comprised of a series of 16 algorithm-generated characters (such as "asdlk8fs9dflku7f") followed by the suffix ".onion." Websites, including hidden services, have system administrator(s) (also called the "admin(s)") who are responsible for overseeing and operating these websites.

Bitcoin

Bitcoin ("BTC") is one type of virtual currency that is circulated over the Internet. BTC is not issued by any government, bank, or company but rather is controlled through computer software. Generally, BTC is sent and received using a BTC "address," which is like a bank account number and is represented by a case-sensitive string of numbers and letters. Each BTC address is controlled through the use of a unique private key, a cryptographic equivalent of a password. Users can operate multiple BTC addresses at any given time, with the possibility of using a unique BTC

address for every transaction.

BTC fluctuates in value. Around March 5, 2018, one BTC was worth approximately $11,573.00. A typical user purchases BTC from a BTC virtual-currency exchange, which is a business that allows customers to trade virtual currencies for conventional money (*e.g.*, U.S. dollars, euros, etc.). Little to no personally identifiable information about the sender or recipient is transmitted in a BTC transaction itself. However, virtual currency exchanges are required by U.S. law to collect identifying information of their customers and verify their clients' identities.

To send BTC to another address, the sender transmits a transaction announcement, cryptographically signed with the sender's private key, across the BTC network. Once the sender's transaction announcement is verified, the transaction is added to the blockchain. The blockchain is a decentralized, public ledger that logs every BTC transaction. In some instances, blockchain analysis can reveal whether multiple BTC addresses are controlled by the same individual or entity. For example, analyzing the data underlying BTC transactions allowed for the creation of large databases that grouped BTC transactions into "clusters." This analysis allowed for the identification of BTC addresses that were involved in transacting with the same addresses.

THE WEBSITE

"The Website" was a website dedicated to the advertisement and distribution of child pornography that operated as a hidden service on the Tor network until March of 2018 when it was seized by law enforcement. The Website was used to host and distribute video files depicting child pornography that could be downloaded by site users. The Website was not intended to be used to upload pornography of adults, as evidenced on the upload page on The Website which clearly stated: "Do not upload adult porn." The Website server had over 250,000 unique video files, which totaled approximately eight terabytes of data.

Any user could create a free account on The Website by creating a username and password.

Only after the user registered an account could the user browse previews of videos available for download and post text to The Website. To download videos from the site, users used "points," which were allocated to users by The Website. A registered user could earn points from The Website in several ways: (1) uploading videos depicting child pornography; (2) referring new users to The Website; (3) paying for a "VIP" account, which lasted for six months, entitled a user to unlimited downloads, and was priced at 0.03 BTC (approximately $327.60 as of March 1, 2018); or (4) paying for points incrementally (*i.e.*, .02 BTC for 230 points). Points were not transferable to any other website or application. Once a customer sent BTC to The Website, the BTC could not be refunded or redirected. The points obtained by the payment of BTC could only be used for downloading videos.

Certain persons joined the conspiracy to distribute child pornography by uploading videos to The Website. Those co-conspirators who uploaded videos of child pornography to The Website for "points" also earned additional "points" each time a customer of the site downloaded that particular video from The Website. Thus, the co-conspirators had a shared goal as part of the conspiracy – increasing the number of unique videos on The Website to drive additional traffic to it, which in turn led to greater downloads and more points for the co-conspirators. When uploading videos, the co-conspirators would use explicit file names highlighting the content as showing the sexual exploitation of minors and would add tags that customers could search for, such as PTHC, 2yo, etc. In order to prevent duplicate videos from being uploaded, The Website operated a digital hash-value check of videos the co-conspirators uploaded in order to compare the video to other videos previously uploaded to the site. The Website did not allow a co-conspirator to upload a video whose hash value matched something previously uploaded to the site.

During the course of the investigation, law enforcement agents in Washington, D.C. accessed The Website on multiple occasions, including on or about September 28, 2017, February

8, 2018, and February 22, 2018, observed its functionality by browsing the listings on The Website, and conducted undercover purchases by downloading child pornography video files from The Website. These downloaded child pornography video files included pre-pubescent children, infants, and toddlers engaged in sexually explicit conduct. Each video available for download from The Website had a title, a description (if added by the co-conspirator), "tags" with further descriptions of the video enabling a user to more easily locate a particular category of video using The Website's search function, and a preview thumbnail image that contained approximately sixteen unique still images from the video.

On or about March 5, 2018, South Korean law enforcement executed a search warrant at the residence of the administrator of The Website in South Korea. Pursuant to the search, South Korean law enforcement seized The Website's server and associated electronic storage media. South Korean law enforcement then provided to U.S. law enforcement a forensic image of the server. U.S. law enforcement subsequently obtained a federal search warrant to review this forensic image.

IDENTIFICATION OF THE DEFENDANT (a/k/a MIKEXP1)

A review of the forensic image of the server revealed a transfer of approximately 0.1 BTC (worth about $38.00) on January 29, 2016 from a BTC address to The Website's BTC address starting with 1BwB. Subpoena returns from a virtual-currency exchange in the United States ("BTC Exchange") revealed that the source of this BTC transfer was from BTC Exchange Account number starting with 528a ("Subject BTC Exchange Account"). The defendant, EZEAGBOR, made that payment to The Website.

Law enforcement's review of the forensic image of the server revealed that The Website created the BTC address starting with 1BwB for a user account in the name of mikexp1. A review of mikexp1's account revealed that between approximately January 28, 2016 and February 19,

2016, mikexp1 downloaded approximately 42 videos from The Website with video file names and descriptions indicative of child pornography. Additionally, from approximately November 25, 2015 to January 25, 2016, mikexp1 uploaded approximately 10 videos of child pornography to The Website. The defendant, EZEAGBOR, downloaded those approximately 42 videos and uploaded those approximately 10 videos, all of child pornography, to The Website.

The videos possessed and uploaded to The Website by the defendant under the moniker mikeexp1 includes video file scara2_00172.avi with file description "Girl." The video is almost fourteen minutes long. The video starts with a message which reads, "13 red my cap so hot" and contains a collage of photographs depicting a clothed female child, approximately ten to thirteen years old, sitting in front of a web camera. The child initially exposes her right breast to the camera and then removes her pants. The child appears to move the camera to face her pubic area and uses her fingers to masturbate her genitalia. Towards the end of the video, the child continues to masturbate herself by using her fingers and also inserts a crayon into her vagina.

Another video possessed and uploaded to The Website by the defendant under the moniker mikeexp1 includes video file scara2_00151.avi with file description "Girl." The video is five minutes and thirty seconds and depicts a nude female child, approximately seven to ten years old. The child is posing in front of a web camera and switches between several sexually suggestive poses, including posing on her hands and knees while she positions her buttocks towards the camera and uses her hands to spread apart her buttocks to expose her genitalia. During the video, the child also sits in a chair facing the camera and spreads her legs to provide a close up view of her pubic area as she uses her fingers to expose her genitalia

Subpoena returns from the BTC Exchange revealed that the Subject BTC Exchange Account (which sent BTC to The Website) was created on or about November 18, 2013 with the following know-your-customer data:

- registered in the name of MICHAEL EZEAGBOR;
- with EZEAGBOR's true date of birth in 1996;
- with EZEAGBOR's true address in Texas;
- using EZEAGBOR's true Social Security number;
- EZEAGBOR's true phone number; and
- an email address of michaelezeagbor@[X].com.

The defendant, EZEAGBOR, created that Subject BTC Exchange Account and funded it from his bank account as described below.

Subpoena returns from Yahoo revealed that the email address of michaelezeagbor@[X].com was created on February 3, 2008 and also is registered to "Mr. Michael Ezeagbor" with the same telephone number that the defendant provided when he created the Subject BTC Exchange Account. The Yahoo account also provided a postal code of 78660, which is the same postal code provided by the defendant when he created the Subject BTC Exchange Account on January 29, 2016.

The Subject BTC Exchange Account was funded by an A+ Federal Credit Union ("A+FCU") checking account ending in 7569 and a A+FCU debit card ending in 2098. Subpoena returns revealed that both of these payment methods were listed in the defendant's name. The subpoena returns further revealed that the defendant opened the account ending in 7569 in 2012. The defendant provided the same date of birth, social security number, home address, and email address when he opened this A+FCU bank account that he had provided to the BTC Exchange when he opened the Subject BTC Exchange Account. Additionally, subsequent law enforcement investigation identified counter security footage from A+FCU on December 4, 2017, which shows an individual resembling the defendant's driver's license photograph accessing his account.

ARREST OF THE DEFENDANT

On January 9, 2019, the defendant was arrested by law enforcement at his residence in the Western District of Texas. At the time of his arrest, the defendant waived his rights and admitted

to accessing The Website and downloading child pornography using the name "mikexp1." Law enforcement also executed a search warrant at the defendant's residence and seized several electronic devices, including computers, data storage devices, and a mobile phone.

A subsequent forensic analysis on the devices seized from the defendant's residence identified approximately 190 images and approximately 14 videos depicting child pornography. The National Center for Missing and Exploited Children (NCMEC) determined that at least 56 images and 2 videos of child pornography depicted at least 8 known child victims.

CONCLUSION

The defendant knowingly possessed one or more computers and electronic devices that contained one or more images and videos of child pornography in digital format, and knowingly possessed said child pornography. These visual depictions of child pornography had been shipped and transported in interstate and foreign commerce and using a means and facility of interstate and foreign commerce, including by computer, and/or were produced using materials that had been shipped and transported in and affecting interstate and foreign commerce, including by computer. The production of these visual depictions involved the use of one or more minors engaging in sexually explicit conduct. The visual depictions of child pornography were of one or more children under the age of eighteen (18) years engaging in such sexually explicit conduct. Specifically:

- One or more images and videos of child pornography possessed by the defendant involved a "prepubescent minor…who had not attained 12 years of age." See U.S.S.G. 2G2.2(b)(2).
- The 10 videos the defendant uploaded to The Website were distributed for the "receipt of a thing of value, but not for pecuniary gain," see U.S.S.G. 2G2.2(b)(3)(B), to wit: the defendant received points that he could only redeem on The Website for downloading additional videos depicting child pornography;

- In total the defendant possessed approximately 190 images and approximately 65 videos depicting child pornography. Accordingly, the offense involved "600 or more images." See U.S.S.G. 2G2.2(b)(7)(D); see also Application Note 4(B)(ii) ("each video…shall be considered to have 75 images.")

II. SENTENCING CALCULATION

A. Statutory Penalties

The offense of Possession of Child Pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B) carries a maximum sentence of 20 years of imprisonment pursuant to 18 U.S.C. § 2252A(b)(2) if any image involved in the offense involved a prepubescent minor or a minor who had not attained 12 years of age, a fine of not more than $250,000 pursuant to 18 U.S.C. § 3571(b), and a term of supervised release – after any period of incarceration – of not less than 5 years or life pursuant to 18 US.C. § 3583(k). In addition, there is a mandatory special assessment for each felony conviction pursuant to 18 U.S.C. § 3013(a)(2)(A).

B. Guidelines Range

The government agrees with the calculation of the defendant's Guidelines sentencing range contained in the pre-sentence report ("PSR"). The base offense level is 18, pursuant to U.S.S.G. § 2G2.2. See PSR ¶ 19. The government agrees with the PSR that several specific offense characteristics apply: the material involved prepubescent minors or minors under the age of 12 (+2); the defendant knowingly engaged in distribution for something of value (+5); the offense involved the use of a computer (+2); and the offense involved more than 600 images (+5). See PSR ¶ 20-23. There are no additional adjustments that apply. Accordingly, the defendant's adjusted offense level is 32. See PSR ¶ 27.

The defendant is entitled to a two-level reduction for acceptance of responsibility pursuant

to U.S.S.G. § 3E1.1(a). See PSR ¶ 29. The government hereby moves to decrease the defendant's offense level by an additional level pursuant to § 3E1.1(b) because he timely notified the authorities of his intention to enter a guilty plea and thus permitted the government and the Court to preserve resources. See PSR ¶ 30. As a result, the defendant's total offense level is 29. See PSR ¶ 31.

The government agrees with the PSR that the defendant has a criminal history score of zero and is in Criminal History Category I. See PSR ¶ 35.

With an offense level of 29 and a Criminal History Category I, the defendant's Guidelines sentencing range is 87 months to 108 months. See PSR ¶ 51.

The defendant has no objections to the PSR's guidelines calculation.

III. GOVERNMENT'S RECOMMENDATION

A. Application of the Federal Sentencing Guidelines

In United States v. Booker, 125 S. Ct. 738 (2005), the Supreme Court held that the mandatory application of the United States Sentencing Guidelines violates the Sixth Amendment principles articulated in Blakely v. Washington, 124 S. Ct. 2531 (2004). As a consequence, the Court invalidated the statutory provision that made the Guidelines mandatory, 18 U.S.C. § 3553(b)(1). Booker, 125 S. Ct. at 756.

In post-Booker cases, the Supreme Court has stated that a district court should begin all sentencing proceedings by correctly calculating the applicable Guidelines range. See United States v. Gall, 552 U.S. 38, 49 (2007) ("As a matter of administration and to secure nationwide consistency, the Guidelines should be the starting point and the initial benchmark."). After giving both parties an opportunity to argue for an appropriate sentence, the district court should then consider all of the applicable factors set forth in 18 U.S.C. § 3553(a). Id. These factors include "the nature and circumstances of the offense and the history and characteristics of the defendant"

(18 U.S.C. § 3553(a)(1)); the need for the sentence imposed to reflect the seriousness of the offense, to provide just punishment for the offense, to afford adequate deterrence to criminal conduct, to protect the public from further crimes of the defendant, and to provide the defendant with needed correctional treatment (18 U.S.C. § 3553(a)(2)); the kinds of sentences available (18 U.S.C. § 3553(a)(3)); the Sentencing Guidelines and related Sentencing Commission policy statements (18 U.S.C. § 3553(a)(4) and (a)(5)); the need to avoid unwarranted sentencing disparities (18 U.S.C. § 3553(a)(6)); and the need to provide restitution to any victims of the offense (18 U.S.C. § 3553(a)(7)).

Notably, the United States Sentencing Commission conducted a hearing on the child pornography sentencing guidelines on February 15, 2012. Department of Justice (DOJ) employees James Fottrell and Steve DeBrota, and former DOJ employee Francey Hakes provided the following testimony regarding how technological advances were exacerbating the threats posed by child pornography offenses:

> In the last ten years, we have seen a sharp increase in the severity and depravity of child pornography offenses, fueled in large part by *swiftly advancing technological changes* which permit offenders to easily store large numbers of images of child sexual abuse, to create safe havens online where they can communicate and bond with other individuals who encourage and promote the sexual exploitation of children, and to utilize sophisticated methods to evade detection by law enforcement. This increase is reflected in the changes in the content of the images over time, as infants and toddlers are now regularly victimized by child pornography offenders and the victims are forced into more brutal and degrading sexual activity.
>
> Additionally, *the technological changes that continue to make it easier for offenders to commit these crimes* are reflected in the number of defendants prosecuted in federal court for child pornography offenses, which has increased every year for over ten years.
>
> We are also seeing the crime change with respect to the *technical complexity and sophistication of the offenders who exploit the developments in both software and hardware*. Storage capacity on hard drives and external media has exploded at the same time that prices for such equipment have dropped,

> making it feasible for individuals cheaply to store millions of image and video files. Internet speeds have skyrocketed, allowing users to download a video in a matter of seconds that, just a few years ago, would have taken hours. At the same time, smart phones and the development of faster wireless networks have turned phones into a viable and portable alternative method to distribute and collect child pornography. *New platforms are being constantly developed to allow individuals to chat, network, and share files. Child pornography offenders are early adopters of these platforms, co-opting them to further their criminal purpose and to create virtual communities that exist outside the bounds of normal society and that embrace and promote the sexual exploitation of children*. Finally, offenders are *exploiting the development of new technologies*, such as evidence eliminating software, encryption, and methods to conceal their Internet activities, *to evade detection by law enforcement*. The result of these changes is clear: we are seeing more and more offenders, engaged in more sophisticated criminal conduct, exploiting a larger number of children in a more depraved way.

See https://www.ussc.gov/sites/default/files/pdf/amendment-process/public-hearings-and-meetings/20120215/Testimony_15_Hakes_DeBrota_Fottrell.pdf (emphasis added).

Moreover, on November 13, 2013, Acting Assistant Attorney General Mythili Raman testified before the Senate Committee on Homeland Security and Governmental Affairs provided the following testimony regarding the unique threat posed by cryptocurrency, including as to child pornography offenses:

> As virtual currency has grown, it has attracted illicit users along with legitimate ones. Our experience has shown that some criminals have exploited virtual currency systems because of the ability of those systems to conduct transfers quickly, securely, and often with a perceived higher level of anonymity than that afforded by traditional financial services. The irreversibility of many virtual currency transactions additionally appeals to a variety of individuals seeking to engage in illicit activity, as does their ability to send funds cross-border.
>
> Cyber criminals were among the first illicit groups to take widespread advantage of virtual currency. We have seen that many players in the cyber underground rely on virtual currency to conduct financial transactions. *Early users of virtual currency also included criminals involved in the trafficking of child pornography*, credit card fraud, identity theft, and high-yield investment schemes. As virtual currency became more widespread and criminals became increasingly computer savvy, other criminal groups moved to capitalize on virtual currency, as well. There are now public examples of virtual currency being used by nearly every type of criminal

> imaginable.
>
> It is not surprising that criminals are drawn to services that allow users to conduct financial transactions while remaining largely anonymous. And, indeed, *some of the criminal activity occurs through online black markets, many of which operate as Tor hidden services.* Tor hidden services are sites accessible only through Tor, an anonymizing network that masks users' Internet traffic by routing it through a series of volunteer servers, called "nodes," across the globe. *Online black markets capitalize on Tor's anonymizing features to offer a wide selection of illicit goods and services, ranging from pornographic images of children* to dangerous narcotics to stolen credit card information.

See https://www.justice.gov/opa/speech/acting-assistant-attorney-general-mythili-raman-testifies-senate-committee-homeland (emphasis added).

B. Basis for the Government's Recommendation

The government submits that a sentence at the low end of the guidelines is appropriate and warranted in this case and specifically recommends a period of supervised release of 10 years based on the factors in 18 U.S.C. § 3553(a). The recommended sentence is sufficient, but not greater than necessary, to accomplish the purposes of sentencing.

1. Nature and Circumstances of the Offense

The defendant specifically sought out and actively participated in an online safe haven that fostered the mutual encouragement and promotion of the sexual exploitation of children. In addition, the defendant laundered funds in a sophisticated manner to support a prolific child pornography website. Consistent with the Justice Department testimony noted above, the defendant's use of cryptocurrency and technologically-advanced online black markets made tracking his activities exponentially more difficult to discover by law enforcement and demonstrates the growing threat posed by such technology in the child exploitation realm. Of specific concern to the government, the defendant not only downloaded these graphic and disturbing videos, but he contributed to the growing marketplace by uploading videos depicting

the sexual abuse of children to The Website.

It goes without saying that child pornography causes real and lasting harm in our society. It is not just about images and videos; it is about real children who are at best being treated as sexualized objects and at worst being horrifically and repeatedly sexually abused. Individuals—like the defendant—who promote child pornography offenses are part of the illicit market for child pornography, which continually re-victimizes the children in already-existing images and videos. As the Supreme Court recognized in the seminal case of New York v. Ferber:

> The use of children as subjects of pornographic materials is very harmful to both the children and the society as a whole. It has been found that sexually exploited children are unable to develop healthy relationships in later life, have sexual dysfunctions, and have a tendency to become sexual abusers as adults.
>
> Pornography poses an even greater threat to the child victim than does sexual abuse or prostitution. Because the child's actions are reduced to a recording, the pornography may haunt him in future years, long after the original misdeed took place.

458 U.S. 747, 758-60 nn. 9 & 10 (1982). The Court continued, "[a] child who has posed for a camera must go through life knowing that the recording is circulating within the mass distribution system for child pornography . . . . It is the fear of exposure and the tension of keeping the act secret that seem to have the most profound emotion repercussions." Id. at 759 n.10. Victims must cope, every day, with wondering whether someone they have come in contact with has seen the pictures or videos of their abuse.

Several of the victims and the parents of victims whose images the defendant possessed submitted victim impact statements, which were provided to defense counsel and probation on July 16, 2019. The victim impact statements share a common theme: the victims must cope, every day, with wondering whether someone they have come in contact with has seen the pictures or videos of their abuse. They are revictimized – continuously exploited – by each consumer of child

pornography. As one of the victims wrote in her Victim Impact Statement:

> Every time someone views this trash, they are once again making me re-live the most horrific part of my childhood. I can never truly heal because the perpetrators and stalkers never allow me to do so. Anyone viewing these videos/pictures is just as guilty for causing me or any other exploited child undue harm, unneeded stress and insecurity in a time when we need to feel safe and have a chance to heal/recover.

Additionally, in the words of a mother of one of the victims:

> Every time a deranged pervert posts and reposts these graphic images of our sons, our nightmare occurs again and again. For I know that someone is deriving sick sexual pleasure from viewing pictures of my sons being raped. Every time that another pervert gets caught with m sons' images, the nightmare occurs all over again, again, and again. Unfortunately, with this, the healing process will never be complete. These pornographic images will always hang over my children's heads and follow them throughout life like a dark cloud. This nightmare could end if these perverts were to stop sharing these photographs but they do not. Instead, they continue to exploit my sons' rapes and abuses by sharing these photographs with other like minded perverts while obtaining their own sexual gratification. The more these photographs are disseminated throughout the Internet the greater the chance that my sons friends and acquaintances could find out about their abuse, victimizing my sons over and over again. I know my sons deserve better than to live under these shadows of fear, undeserved guilt, shame, and self-loathing.

Accordingly, the defendant participated in and fueled this exploitative industry, as evident by both his downloads and uploads of videos depicting child pornography to The Website. Although the defendant has pled guilty to possessing videos of child pornography, his conduct depicts an individual who was not only a possessor, but one who trafficked in videos of children being sexually abused.

2. History and Characteristics of the Defendant

In most criminal cases, a defendant will appear for sentencing and offer mitigating evidence, asking the Court to consider the defendant's sometimes less obvious, but positive attributes. In child-exploitation related crimes, however, a defendant's good qualities are frequently the easiest to see. Defendants appear to be like any other law-abiding citizen—they work, worship, and have the support of their families. Their crimes against children, and the

reasons they commit them, have been hidden from colleagues, friends, and loved ones. Despite that fact, the perpetrator's private crime is a horrific one, and offenders must be held accountable for the damage they have done.

Here, the defendant has no criminal record. He indicated relatively soon after he was charged a desire to accept responsibility and plead guilty in this case. He has been diagnosed with Autism, Anxiety, and Depression and continues with mental health treatment presently. PSR ¶ 43. However, the government has already taken these mitigating mental health factors into account when the government extended a plea to Possession of Child Pornography in lieu of Conspiracy to Distribute Child Pornography and is recommending a sentence at the low end of the guidelines.

3. Punishment, Deterrence, Protection, and Correction

A sentencing court "shall impose a sentenced sufficient, but not greater than necessary" to comply with the need for a sentence: "(A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense; (B) to afford adequate deterrence to criminal conduct; (C) to protect the public from further crimes of the defendant; and (d) to provide the defendant with needed educational or vocational training, medical care, or other correctional treatment in the most effective manner." 18 U.S.C. § 3553(a)(2).

The government's recommended sentence is sufficient, but not greater than necessary, to provide just punishment for the defendant's offenses. The defendant's possession and distribution of child pornography videos and resulting promotion of a child exploitation scheme harmed society at large and specifically, child victims, and thus warrants a sentence of imprisonment. Moreover, a term of supervised release with conditions including sex offender assessment and treatment is important to ensuring that the defendant receives the continuing treatment and support that will ensure he does not commit any additional crimes in the future.

4. Available Sentences And Supervised Release Conditions

The defendant should be sentenced to a term of incarceration. The defendant is in Zone D of the Guidelines, and thus a probationary sentence would be a departure from the Guidelines. PSR ¶ 56.

In addition, the Court should impose a term of supervised release, and the government recommends a term of 10 years. Supervised release is critical because it will subject the defendant to ongoing monitoring and ensure that he does not revert back to his criminal conduct when he finds himself facing a life challenge or obstacle.

The conditions of supervised release should include the following conditions, which are conditions imposed in similar child exploitation cases and conditions:

(1) The defendant must submit to searches of his person, property, house, residence, vehicle, papers, computers, other electronic communications or data storage devices or media, and effects, at any time, with or without a warrant, by law enforcement or probation officer with reasonable suspicion concerning unlawful conduct or a violation of a condition of supervision.

(2) The defendant must undergo and comply with sex offender evaluation and treatment. This may include the use of polygraph testing as part of the therapeutic process.

(3) The defendant's use of the Internet, computers, and any other Internet-capable devices will be restricted and monitored.

(4) The defendant will not have direct contact with minors without the written approval of probation. This also entails both an employment/volunteer restriction and residential restriction, in that the defendant shall not be employed in any capacity, or participate in any volunteer activity, which may cause him to come in direct

and/or unsupervised contact with children for more than momentary duration without advanced approval by the United States Probation Office, and the defendant shall have all residences pre-approved by the United States Probation Office. Specifically, the defendant shall not live in a residence where minor children also reside without the permission of the United States Probation Office.

As it relates to the above conditions, first, the defendant will be required by statute to register as a sex offender as a result of his conviction in this case. Second, the defendant's crimes stem from his online communications. Thus, the defendant's use of the Internet to commit his crimes justifies monitoring his future use. Third, the defendant's collection and distribution of child pornography material justifies monitoring his direct contact with any minors and supports the imposition of sex offender evaluation and continued sex offender treatment.

5. Avoiding Unwarranted Sentencing Disparity

One of the statutory factors to consider at sentencing is the need to avoid unwarranted disparity. Indeed, avoiding such uncertainty and disparity was one of the purposes for the creation of the Sentencing Guidelines. No similarly situated defendants have been sentenced in this matter in this Court. In the United States District Court for the District of Columbia, two users of The Website have been sentenced, but these defendants were not uploaders to the site. One pled guilty to Money Laundering (due to evidentiary issues associated with that specific case) and was sentenced to 18 months incarceration, and the other pled guilty to Receipt of Child Pornography (second offense) and was sentenced to 15 years incarceration. It should be noted that neither of these users uploaded illicit content to The Website in contrast to the defendant here, who was both a user and distributor on the site. However, it is without dispute that the defendant here indicated early on that he accepted responsibility and wished to plead guilty. Accordingly, the government's recommendation, at the low end of a guideline sentence, is appropriate based on the factors

presented in this case.

6. Restitution and Victim Impact Statements for the Victims

The government has been in communication with the victims' lawyers and defense counsel. At the time of this filing, the victim identified in the "At School" series (known as 'Violet") has requested restitution. It is the government's understanding that the parties are in the process of negotiating a restitution amount for "Violet." This amount will be subsequently included in any Judgement and Commitment Order by the Court at the time of sentencing. The government acknowledges and is appreciative of the defendant's willingness to cooperate with his restitution obligations without the need for protracted litigation in Court.

IV. CONCLUSION

WHEREFORE, based on the facts of this case, the information contained in the Presentence Investigation Report, and the foregoing, the government recommends that the Court sentence the defendant to a term of imprisonment at the low end of the applicable guideline range, to be followed by 10 years of supervised release, with the standard and recommended conditions of supervision.

Respectfully submitted,

JESSIE K. LIU
United States Attorney
District of Columbia

By: */s/ Lindsay Jill Suttenberg*
LINDSAY JILL SUTTENBERG
Assistant United States Attorney

JOHN F. BASH
United States Attorney
Western District of Texas

/s/ Matthew Devlin

By: _____
MATTHEW DEVLIN
Assistant United States Attorney

CERTIFICATE OF SERVICE

I hereby certify that on September 11, 2019, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system which will send notification of such filing to the following:

David M.C. Peterson, Esq.
Assistant Federal Public Defender
504 Lavaca Street, Suite 960
Austin, Texas 78701
(512) 916-5025
Fax (512) 916-5035
California Bar No. 254498
Attorney for Defendant

/s/ Matthew Devlin

_____
MATTHEW DEVLIN
Assistant United States Attorney